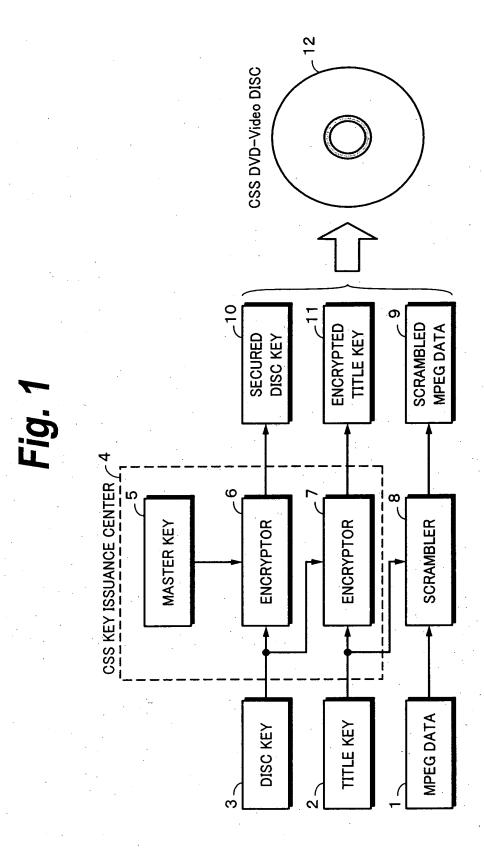
$\sum_{i=1}^{n}$ 



Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 3 of 49

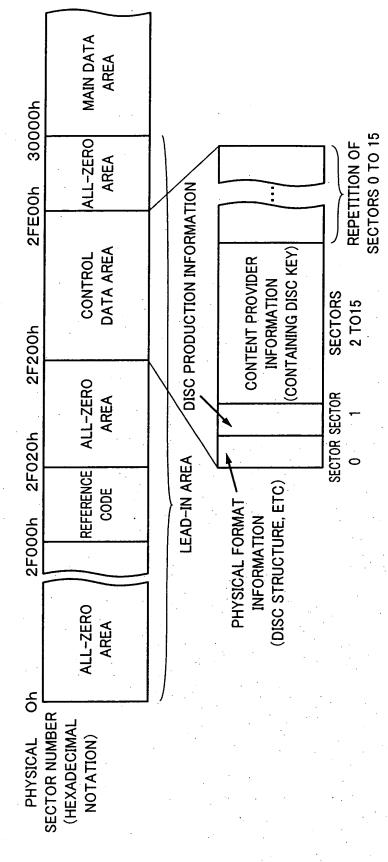


Fig. 4

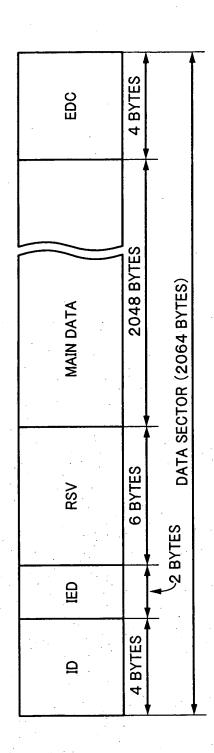


Fig. 5

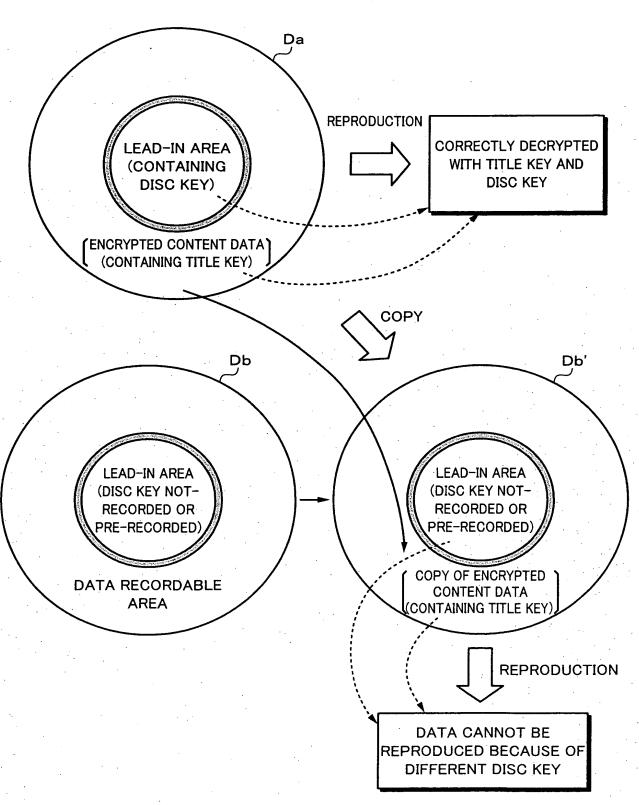
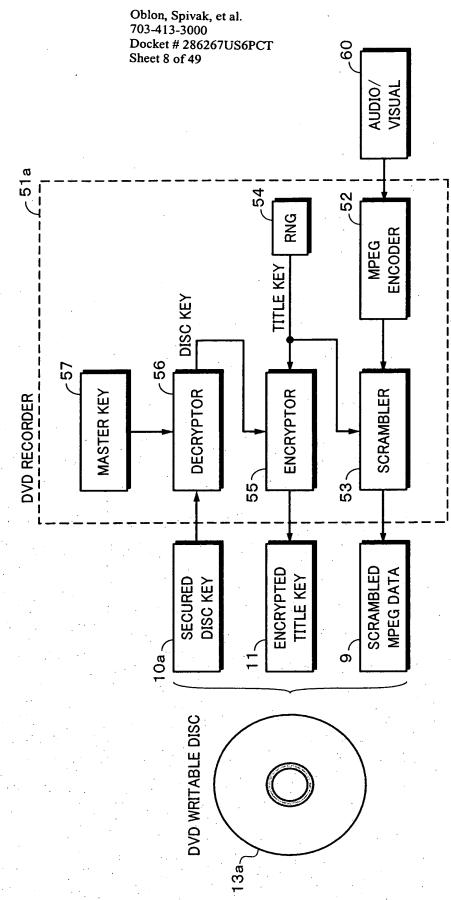


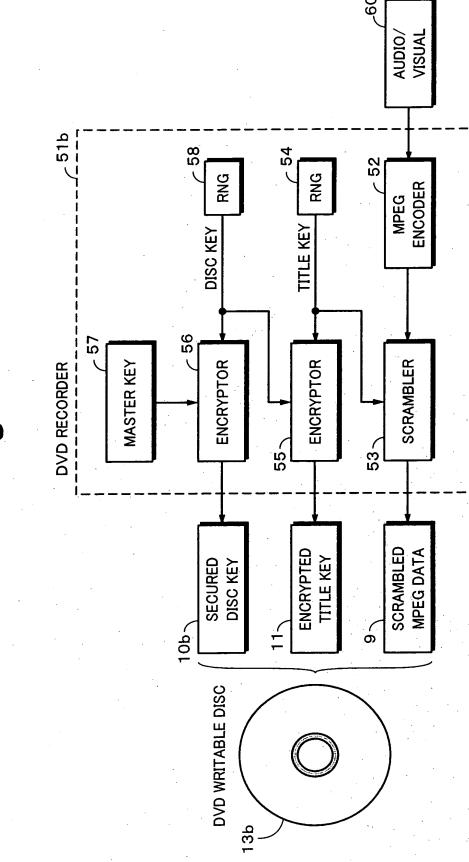
Fig. 6

Fig. 7

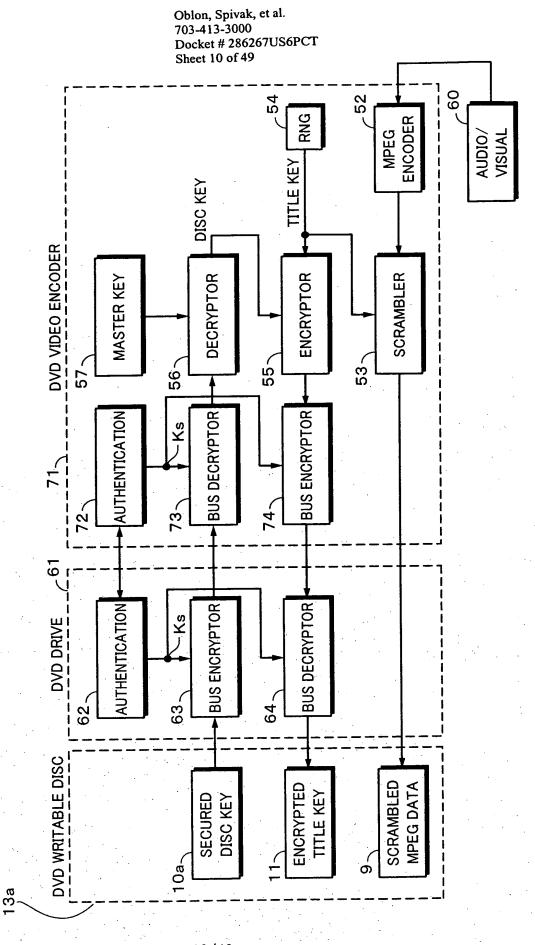
| 41<br>ST                     |                                    |                          |  |                                   |                                     |                           |                          |   |
|------------------------------|------------------------------------|--------------------------|--|-----------------------------------|-------------------------------------|---------------------------|--------------------------|---|
| PC 41<br>(HOST)              | S1                                 | . S3                     | y,   | \$7                               | \$10                                | \$11                      | \$14                     |   |
| IVE 31                       | AKE                                | REQUEST SECURED DISC KEY | RETURN SECURED DISC KEY<br>ENCRYPTED WITH Ks | REQUE                             | RETURN ENCRYPTED TITLE KEY AND CGMS | REQUEST SCRAMBLED CONTENT | RETURN SCRAMBLED CONTENT |   |
| DVD DRIVE 31                 | . S2                               | . S4                     | . S5   | MS S8                             | 89                                  | \$12                      | \$13                     |   |
| RAMBLED<br>DIUM 12           | SEEK AND READ<br>CONTENT DATA ZONE | READ SECURED DISC KEY    | SECURED DISC KEY                             | READ ENCRYPTED TITLE KEY AND CGMS | ENCRYPTED TITLE KEY AND CGMS        | READ SCRAMBLED CONTENT    | SCRAMBLED CONTENT        |   |
| CSS SCRAMBLE<br>DVD MEDIUM 1 |                                    |                          |  |                                   |                                     |                           |                          | · |

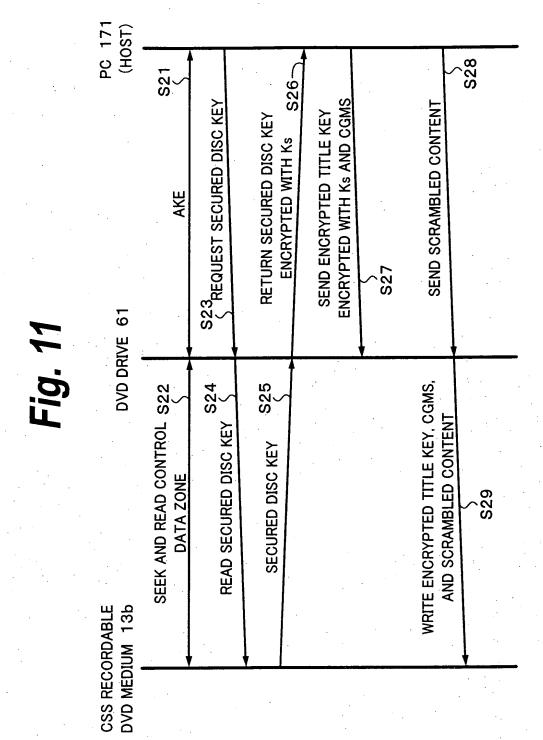


8/49



9/49







3b

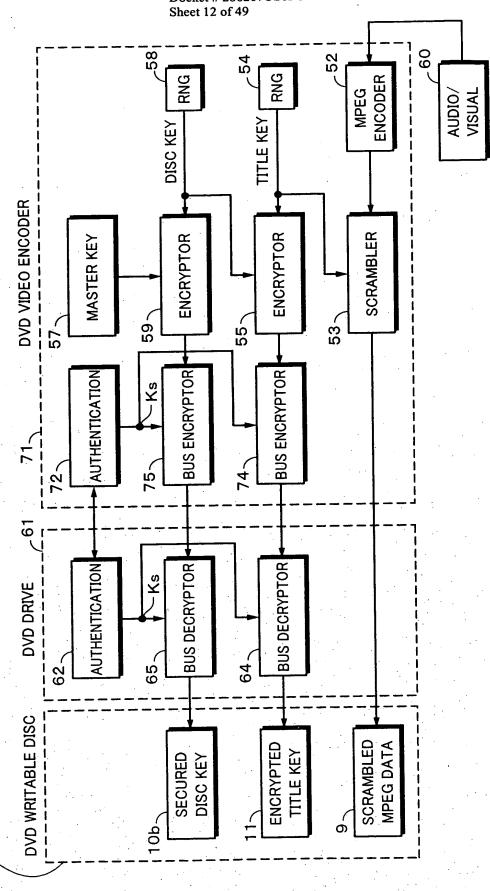
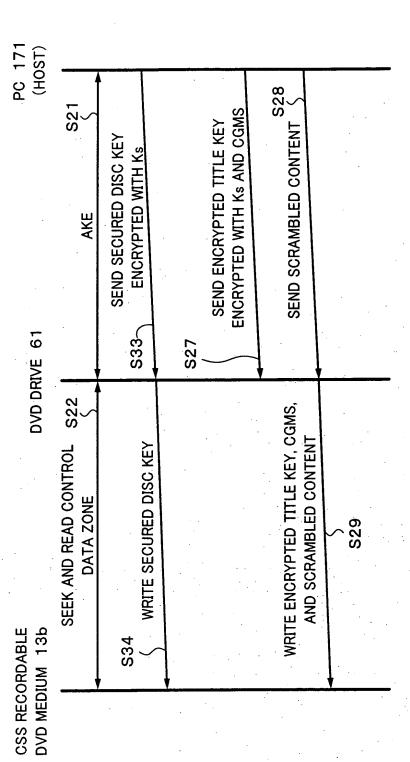
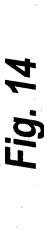


Fig. 13





3a

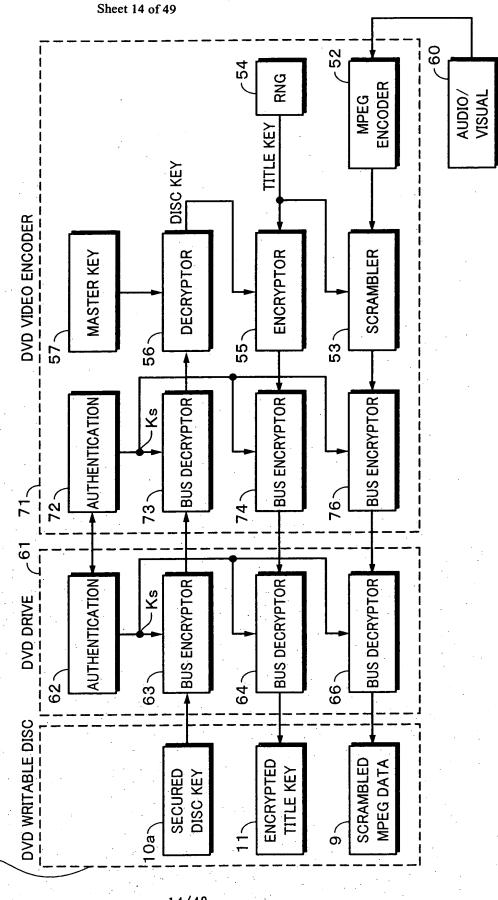
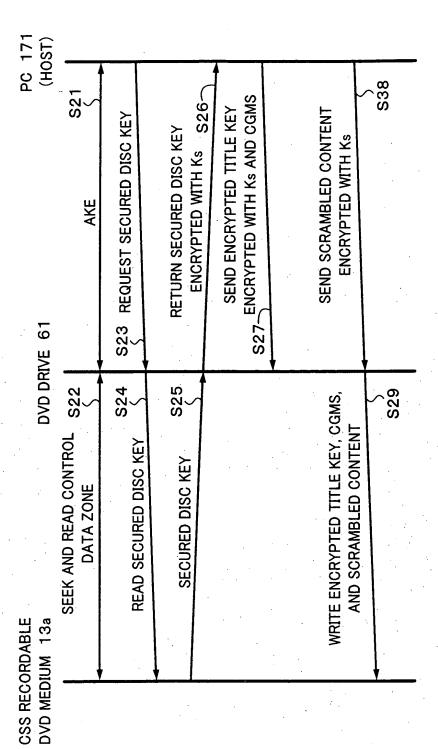
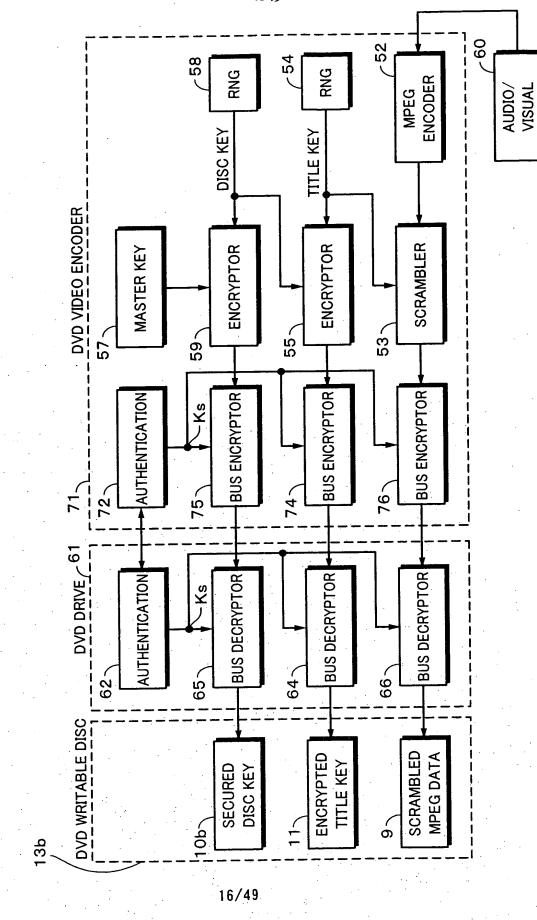


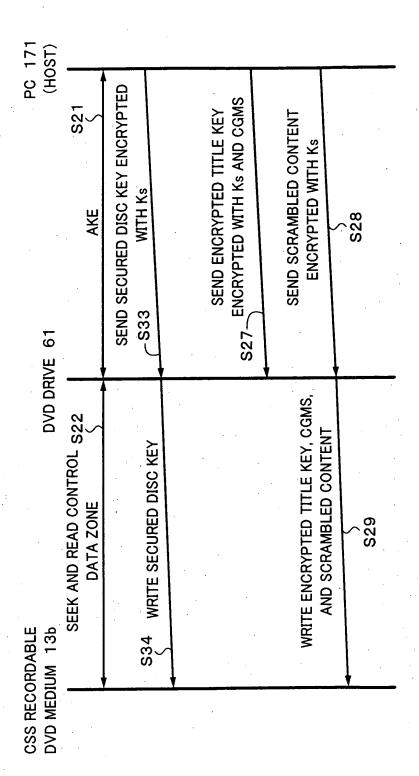
Fig. 15





.

Fig. 17



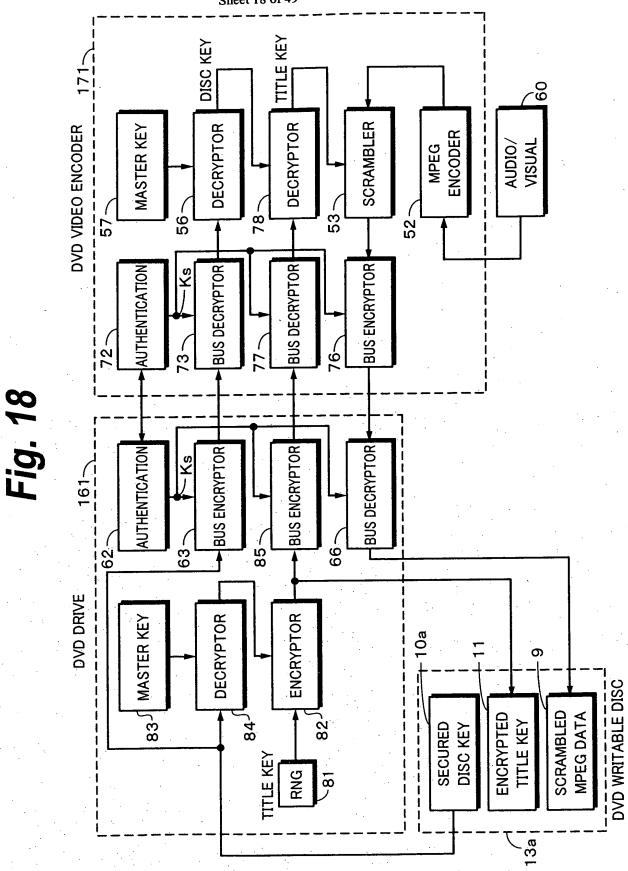
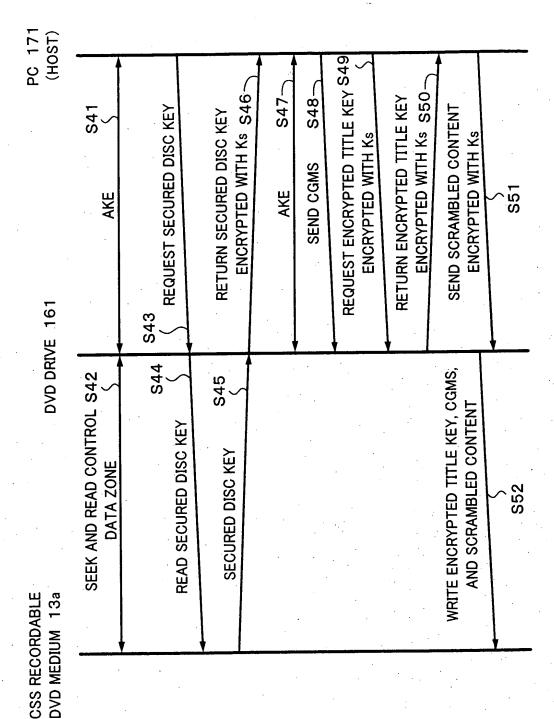


Fig. 19



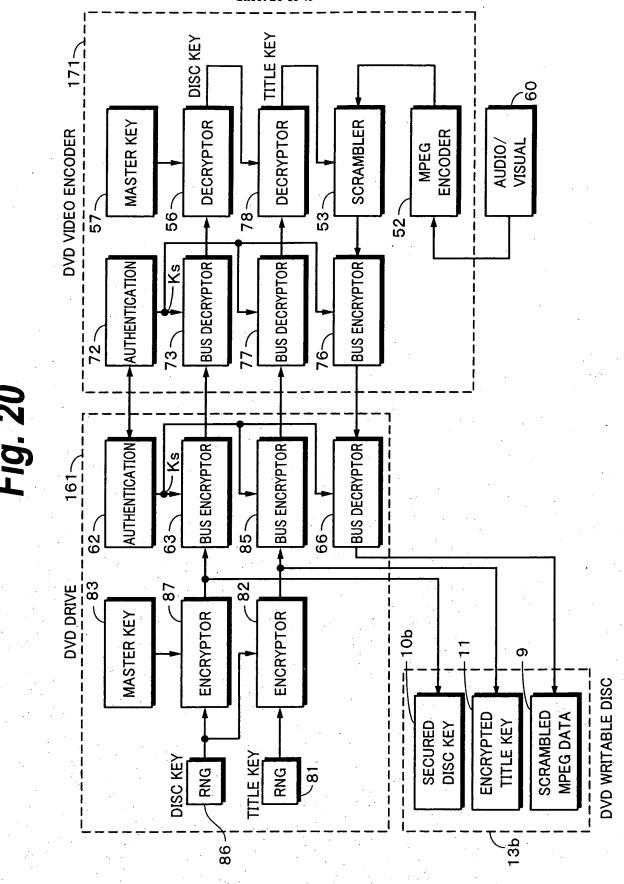
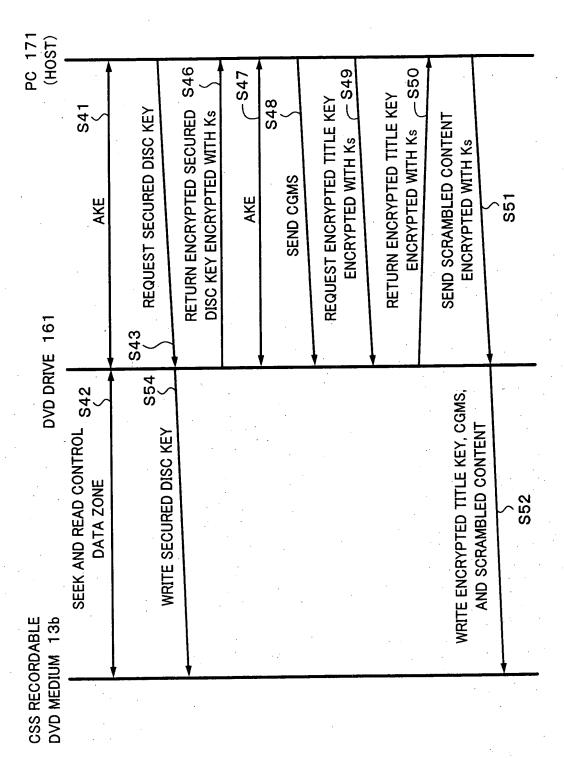
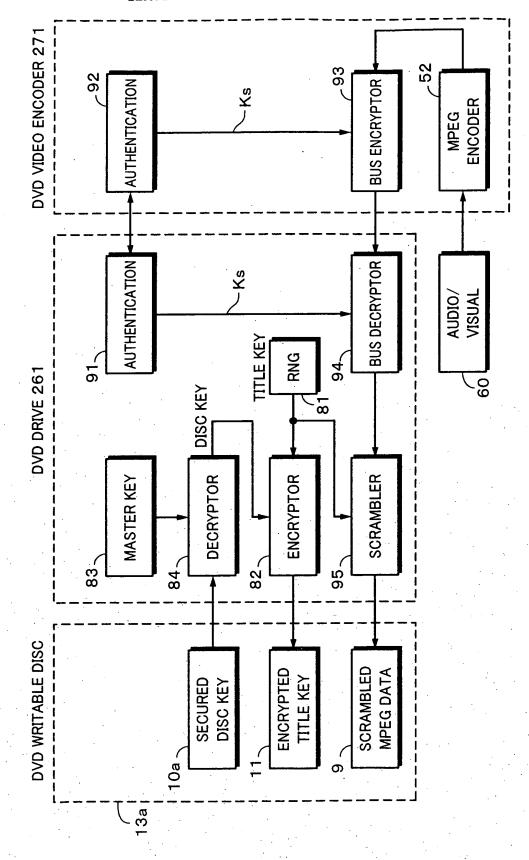
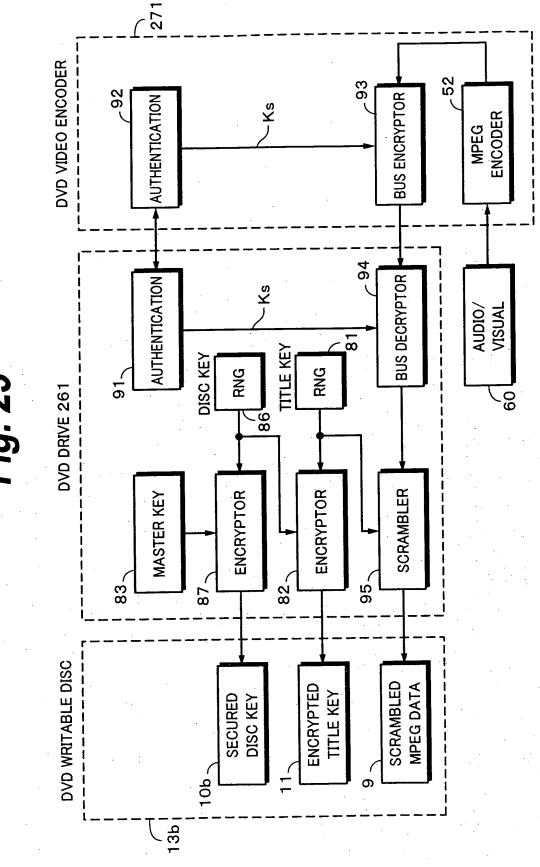


Fig. 21



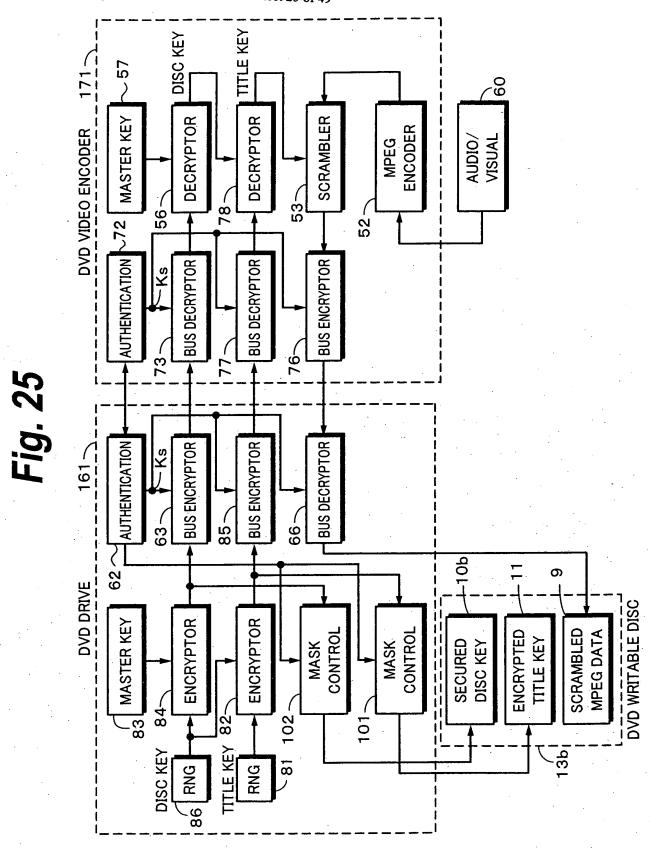




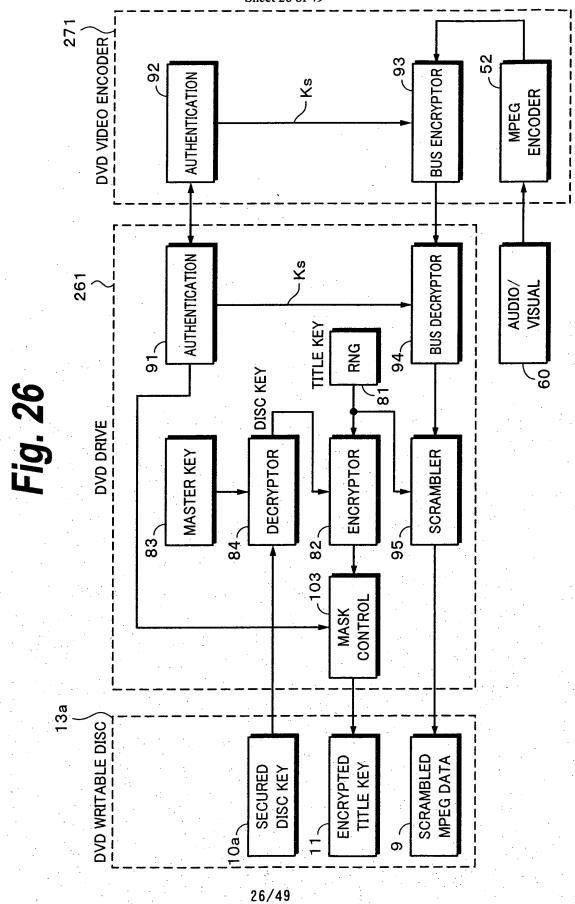
23/49

24/49

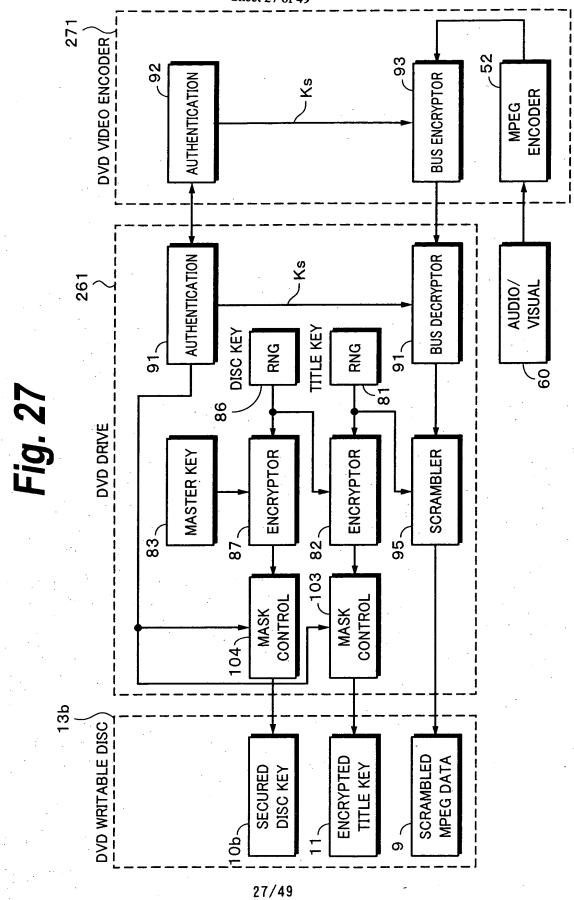
Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 25 of 49

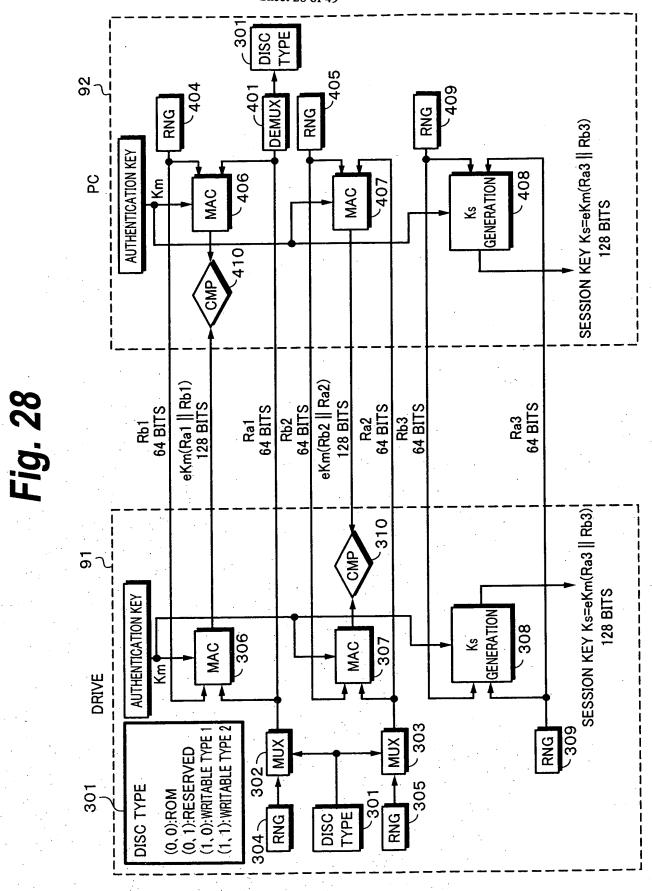


Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 26 of 49



Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 27 of 49





28/49

Fig. 29

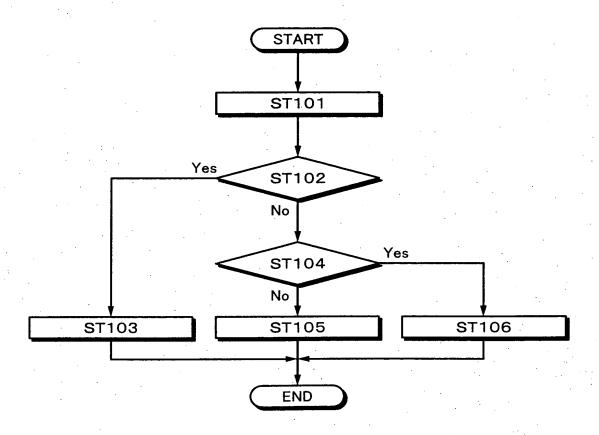
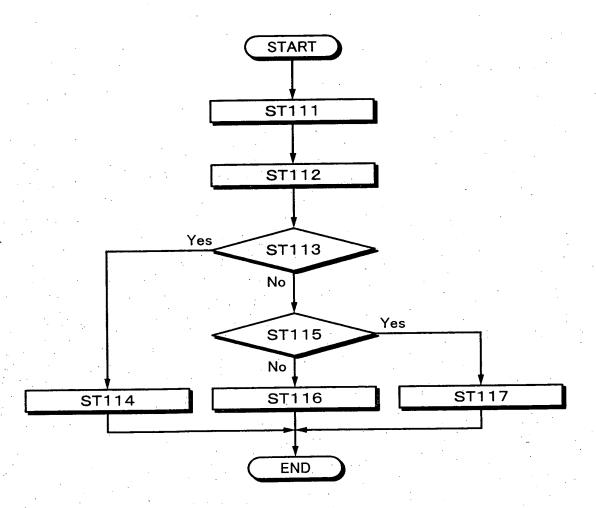
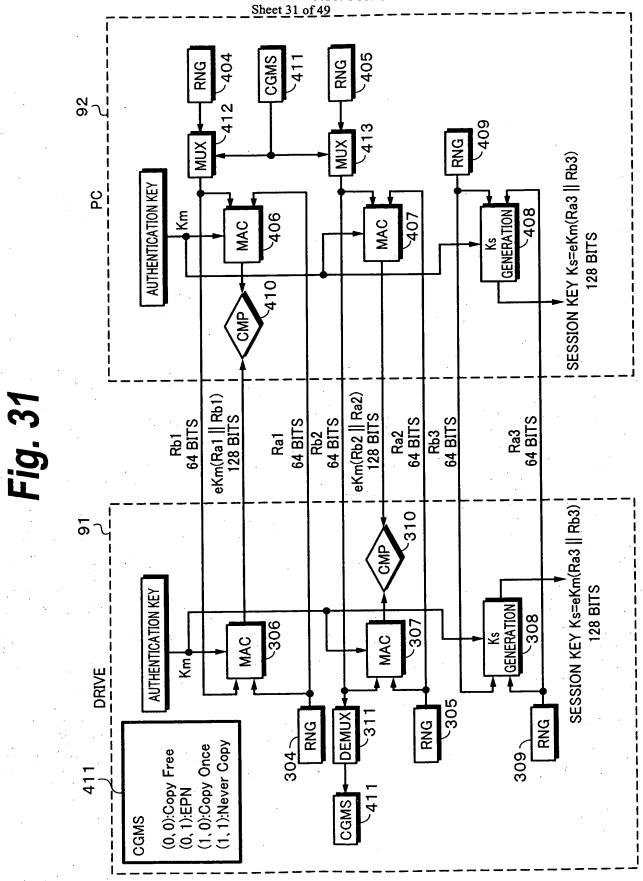


Fig. 30





## Fig. 32

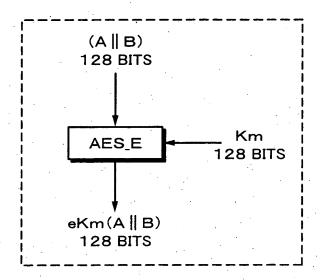


Fig. 33

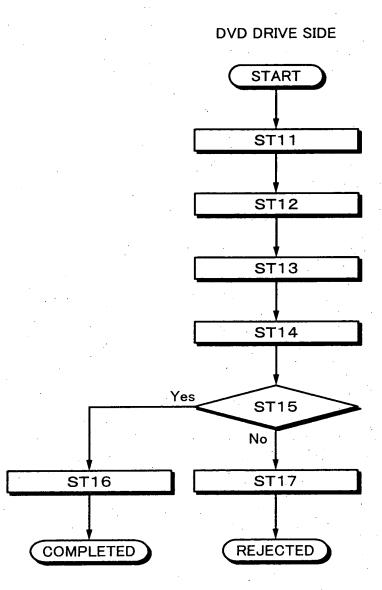
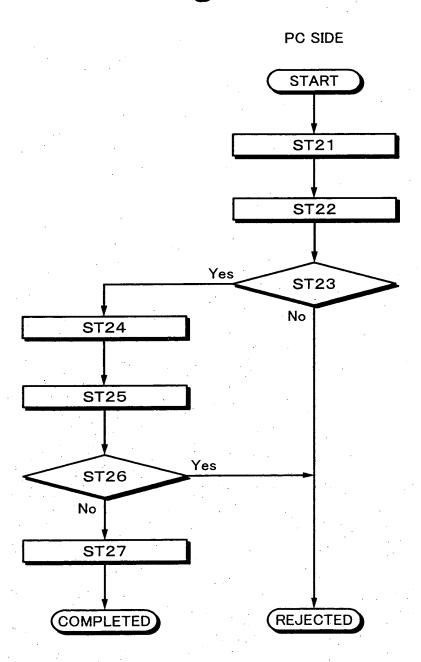


Fig. 34

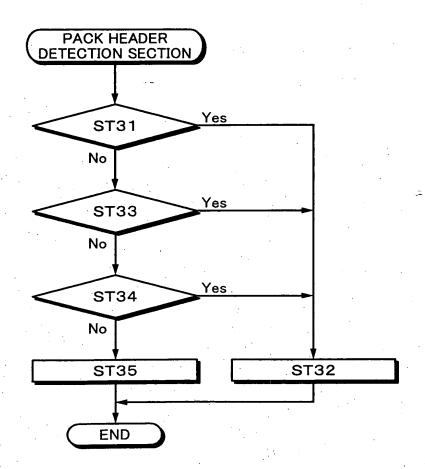


Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 35 of 49

SECTOR DATA AV PACK DETECTION 501 BUS ENCRYPTOR AV DATA ENCRYPTOR **SESSION KEY** AV PACK DETECTION 511 **BUS DECRYPTOR** 512~ AV DATA DECRYPTOR SESSION KEY 514 SECTOR DATA 2KB

Fig. 35

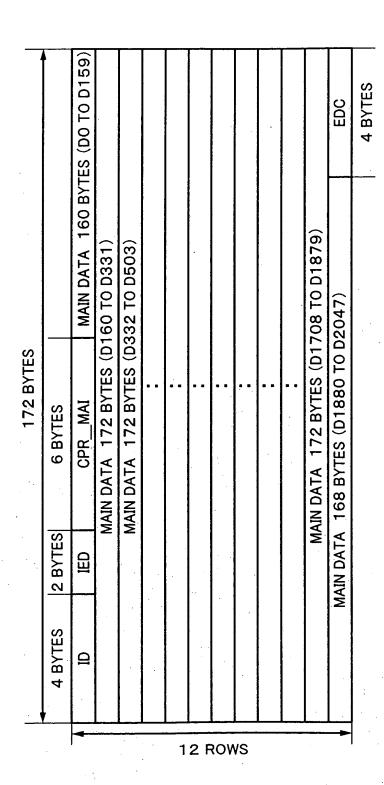
Fig. 36



# Fig. 37

| VIDEO, AUDIO, OR SUB PICTURE | AREA ENCRYPTED / DECRYPTED | 1920 BYTES |
|------------------------------|----------------------------|------------|
| VIDEC                        | тер                        |            |
| PACK HEADER PACKET HEADER    | :NCRYPTED / DECRYPTED      | 128 BYTES  |
| PACK HEADER                  | AREA NOT ENCRYPT           |            |

Fig. 38



**EXAMPLE OF STRUCTURE OF SECTOR** 

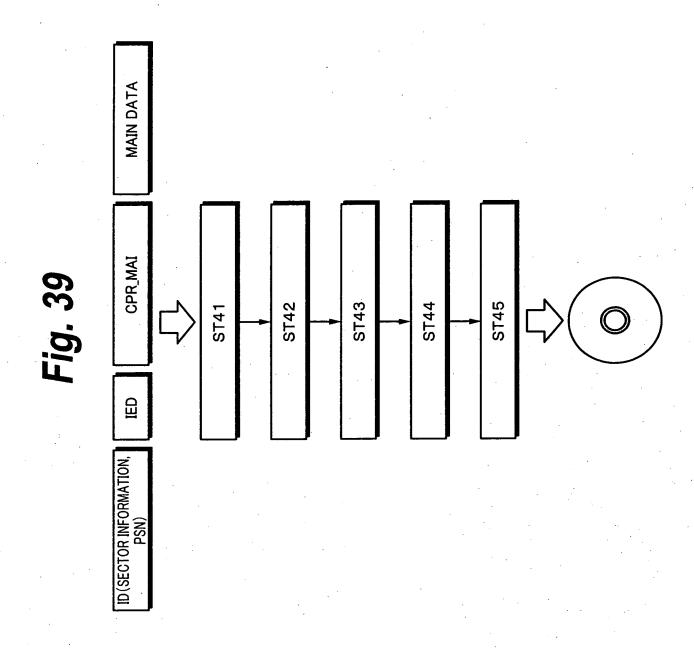
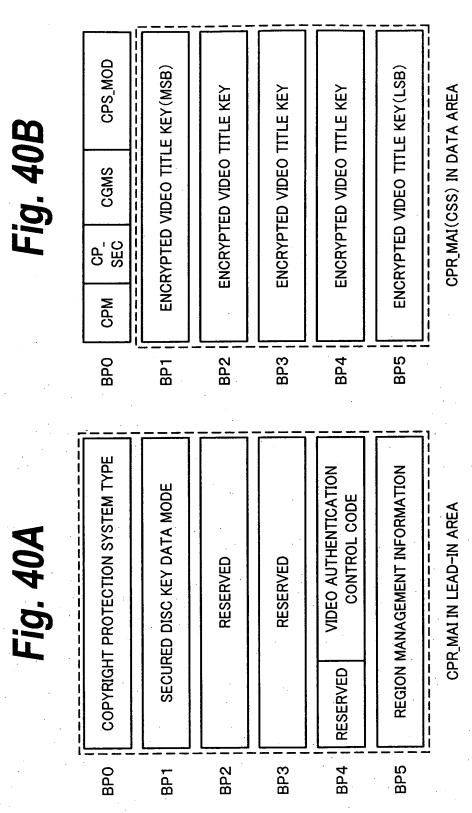


Fig. 40A

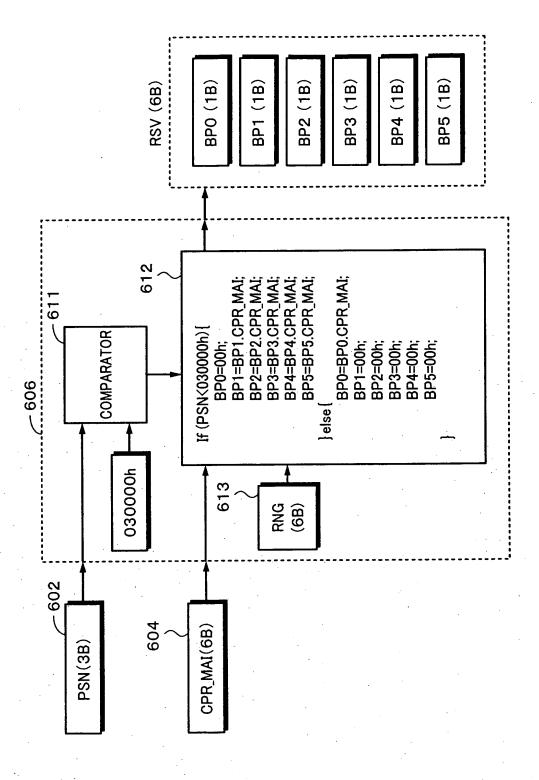


··· MASKING AREA

EDC(4B) EDC CALCULATION MIXER IED(2B) RSV(6B) -809 603 IED CALCULATION CPR\_MAI FILTER 909 INFORMATION (1B) MAIN DATA (2KB) CPR\_MAI (6B) SECTOR PSN(3B) 604~ 605~ 602~

41/49

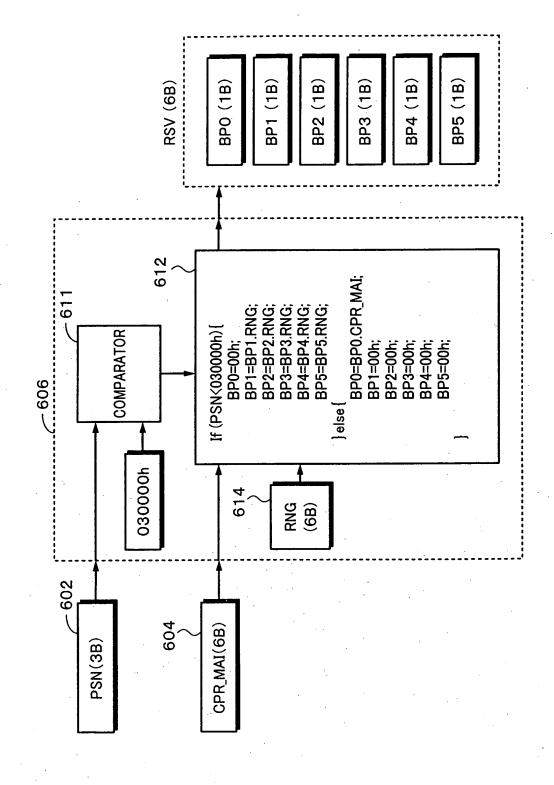
Fig. 42



(1B) (1B) BP4 (1B) BP5 (1B) BP1 (1B) BP0 (1B) **RSV (6B)** BP2 врз 612 BP0=BP0.CPR\_MAI; BP1=BP1.RNG; BP2=BP2.RNG; BP3=BP3.RNG; BP4=BP4.RNG; BP2=BP2.CPR\_MAI; BP3=BP3.CPR\_MAI; BP4=BP4.CPR\_MAI; BP5=BP5.CPR\_MAI; If (PSN<030000h){
BP0=BP0.CPR\_MAI;
BP1=BP1.CPR\_MAI; 611 COMPARATOR 909 030000h 614 RNG (6B) 602 604 CPR\_MAI(6B) PSN(3B)

43/49

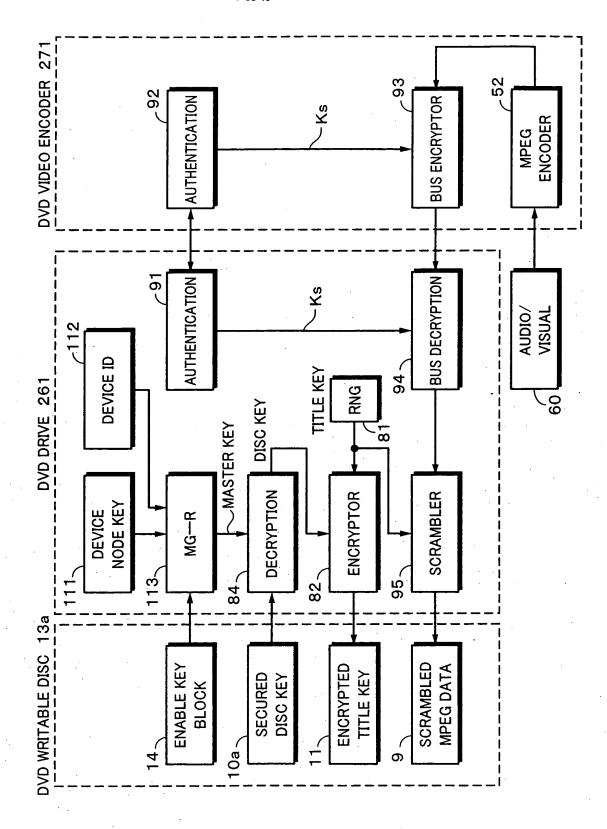
Fig. 44



ST58 **ST59 ST57 ERASURE OF SESSION KEY** Yes **ST63 ST56 ST62** ST60 ST61 **(19)** GENERATION OF SESSION KEY ST52 ST53 **ST55** ST54 **ST51 (II)** ŝ ŝ å

45/49

Fig. 46



Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 47 of 49

### DESCRIPTION OF REFERENCE NUMERALS

| ST101 | DETERMINATION OF MEDIUM TYPE                  |
|-------|---|
| ST102 | ROM ?   |
| ST103 | DISC TYPE = ROM                               |
| ST104 | DISC APPLICATION CODE = VIDEO WRITABLE ?      |
| ST105 | DISC TYPE = RESERVED                          |
| ST106 | DISC TYPE = VIDEO WRITABLE                    |
|       |   |
| ST111 | MUTUAL AUTHENTICATION                         |
| ST112 | OBTAIN DISC TYPE FROM DRIVE.                  |
| ST113 | DISC TYPE = ROM ?                             |
| ST114 | PROHIBIT DATA FROM BEING WRITTEN              |
| ST115 | DISC TYPE = VIDEO WRITABLE                    |
| ST116 | DATA WRITABLE                                 |
| ST117 | VIDEO WRITABLE CORRESPONDING TO CSS/CPRM      |
|       |   |
| ST11  | RECEIVE (Rb1, Rb2)                            |
| ST12  | RETURN (eKm (Ra1   Rb1), Ra1)                 |
| ST13  | RETURN (Ra2, Ra3)                             |
| ST14  | RECEIVE (eKm (Rb2    Ra2), Rb3)               |
| ST15  | SAME MAC ?                                    |
| ST16  | ESTABLISHMENT OF SESSION KEY (eKm (Ra3   Rb3) |
| ST17  | RETURN (ERROR)                                |

Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT. Sheet 48 of 49

| ST21 | SEND KEY (Rb1, Rb2)                                 |
|------|---|
| ST22 | REPORT KEY (eKm (Ra1   Rb1), Ra1)                   |
| ST23 | SAME MAC ?  |
| ST24 | REPORT KEY (Ra2, Ra3)                               |
| ST25 | SEND KEY (eKm (Rb2     Ra2), Rb3)                   |
| ST26 | ERROR ?   |
| ST27 | ESTABLISHMENT OF SESSION KEY (eKm (Ra3   Rb3)       |
|      |   |
| ST31 | VIDEO PACK  |
| ST32 | ENCRYPT/DECRYPT DATA.                               |
| ST33 | AUDIO PACK  |
| ST34 | SUB PICTURE PACK                                    |
| ST35 | DOES NOT ENCRYPT/DECRYPT DATA.                      |
|      |   |
| ST41 | ADD EDC.  |
| ST42 | SCRAMBLE MAIN DATA.                                 |
| ST43 | ENCODE DATA WITH ECC.                               |
| ST44 | INTERLEAVE 16 ROWS OF PO.                           |
| ST45 | MODULATE 26 SYNC FRAMES PER SECTOR.                 |
|      |   |
| ST51 | HAS DVD+RW/+R DISC BEEN INSERTED ?                  |
| ST52 | HAS PC APPLICATION BEEN STARTED ?                   |
| ST53 | MUTUAL AUTHENTICATION AND GENERATION OF SESSION KEY |
| ST54 | COMPLETED ?   |
| ST55 | DISABLE CSS KEY WRITE PROHIBITION                   |
| ST56 | COMPLETION OF PC APPLICATION ?                      |
|      |   |

48/49

Oblon, Spivak, et al. 703-413-3000 Docket # 286267US6PCT Sheet 49 of 49

|            | Sheet 49 of 49                        |
|------------|---------------------------------------|
| ST57       | ERASE SESSION KEY GENERATED IN PC.    |
| ST58       | HAS PC APPLICATION BEEN STARTED ?     |
| ST59       | HAS DVD+RW/+R DISC BEEN EJECTED ?     |
| ST60       | ERASE SESSION KEY GENERATED IN DRIVE. |
| ST61       | PROHIBIT CSS KEY FROM BEING WRITTEN.  |
|            |                                       |
| 9          | SCRAMBLED MPEG DATA                   |
| 10a, 10b   | SECURED DISC KEY                      |
| 11         | ENCRYPTED TITLE KEY                   |
| 13a, 13b   | WRITABLE DISC                         |
| 52         | MPEG ENCODER                          |
| 53, 95     | SCRAMBLER                             |
| 56, 78, 84 | DECRYPTOR                             |
| 57, 83     | MASTER KEY                            |
| 60         | AUDIO/VISUAL DATA                     |
| 62, 72     | AUTHENTICATION SECTION                |
| 63, 76, 85 | BUS ENCRYPTOR                         |
| 66, 73, 77 | BUS DECRYPTOR                         |
| 81, 86     | RANDOM NUMBER GENERATOR               |
| 82, 87     | ENCRYPTOR                             |
| 101, 102   | MASK CONTROL                          |
| 161, 261   | DRIVE                                 |

171, 271

PC

# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

#### **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

| Defects in the images include but are not limited to the items checked: |  |  |
|---|--|--|
| ☐ BLACK BORDERS   |  |  |
| ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES                                 |  |  |
| ☐ FADED TEXT OR DRAWING   |  |  |
| ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING                                  |  |  |
| ☐ SKEWED/SLANTED IMAGES   |  |  |
| ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS                                  |  |  |
| ☐ GRAY SCALE DOCUMENTS  |  |  |
| LINES OR MARKS ON ORIGINAL DOCUMENT                                     |  |  |
| ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY                 |  |  |

## IMAGES ARE BEST AVAILABLE COPY.

OTHER:

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.